WORLD WIDE WEB FOUNDATION

1110 Vermont Avenue NW, Suite 500
Washington DC, 20005 USA
www.webfoundation.org

28 September 2017

VIA ELECTRONIC FILING

Marlene H. Dortch,
Secretary Federal Communications Commission
445 12th Street, SW Washington, DC 20554

Re: In the Matter of "Restoring Internet Freedom" - WC Docket No. 17-108

On September 25, 2017, Tim Berners-Lee and Adrian Lovett, CEO and President of Web Foundation ("Web Foundation") met with the Chairman of the FCC, Ajit Pai, and Jay Schwartz, Wireline Advisor of the FCC.

During the meeting, we discussed how the US has historically been a champion of internet freedom worldwide, and its regulatory frameworks are usually perceived as precedents to be followed. We stressed that the web has been a key space for innovation, economic growth and freedom of speech. We underlined that these developments were only possible because the markets for access and content were separate. We claimed that rules to enforce the net neutrality principles (no blocking, no throttling, and no paid prioritization), such as those included in the 2015 Open Internet Order, have become necessary for these markets to continue following the virtuous circle of growth. We had previously presented some of these arguments in a previous submission by the Web Foundation[1].

Regarding some of the questions raised during our meeting, we wanted to respond in greater detail. Our response is provided at the end of this document.

Please direct any questions to the undersigned.

Respectfully Submitted,

Adrian Lovett
President & CEO
Web Foundation

[1] https://ecfsapi.fcc.gov/file/10717560630144/World_Wide_Web_Foundation_Comments_on_Net_Neutrality_Submitted_to_FCC_July2017.pdf

Detailed responses:

Why do we need rules now and yet the web managed to thrive before any rules were in place?

Many things have changed over the past decades. Two key changes I would like to highlight are the incentives to discriminate, and the power to exercise such discrimination effectively.

- Incentives: the growth of the internet has enabled a robust economy on the content layer. ISPs, following short-term incentives, might be interested in extracting part of the value available on that layer. The strength of these incentives has grown in proportion to the size of the economy ISPs act as gatekeepers to.

- Power: technology developed for traffic management purposes (e.g. Deep Packet Inspection) has provided ISPs with a tool to effectively discriminate traffic, and thus act upon these short-term incentives.

At the Web Foundation we consider that the role of policy-makers is to design a structure of incentives such that all key actors of an ecosystem are focusing on its long-term sustainability and growth. We believe the strong rules against traffic discrimination play this role, and are key to enabling the continuation of the virtuous circle that has provided economic benefits for both the content and the infrastructure layers of the internet.

Can encryption help circumvent traffic discrimination?

The core issue with traffic discrimination is that generates distortions. These distortions have long-term impact of the impact on the ecosystem of content producers. It is more of a systemic problem than an individual problem, much like subsidizing certain companies, and not its competitors is for the markets of goods and services. As long as a relevant percentage of the population experiences the internet through an ISP that discriminates against certain content, then all consumers suffer the consequences from these distortions. The solution to this systemic problem needs to impact on the whole system: for example with a general rule that ensures no traffic discrimination.

To address the question as such: at some point a router in the network has to be shown a URL that points to the server where the content to be retrieved is hosted. Services like TOR and proxy servers mask the identity of the user by splitting the network into two parts:

- one between the user and the proxy server that knows the user's identity but doesn't know the actual content that is being sought (is told the proxy server is the "final destination")

- another between the proxy server and the server that hosts the content to be retrieved that knows the content but thinks the proxy server is the retrieving agent.

Therefore these tools could theoretically work to circumvent traffic discrimination in scenarios in which these two sections of the network are managed by different ISPs and only the one that manages the first section discriminates against the website of interest. Relying on proxy servers to avoid traffic discrimination would require ISPs to be transparent about which websites or protocols are being discriminated, and the creation of something like a "dark domain name system" architecture for proxy servers to map the Content Delivery Networks hosting available copies of the data and the dark routes that should be chosen in order to avoid throttling once they unmask the final destination. This would of course be hugely inefficient. Nevertheless, the key weakness of the approach is that given the existing technology ISPs could easily identify the proxy servers used as middle points. In some countries ISPs throttle traffic heading towards proxy servers as a way to disincentivize their use, or block them completely.

Encryption and proxy servers are popular tools amongst users that seek to control how much of their data they will allow intermediaries to capture. As we build our digital identities online, this can be equated to people's right to determine their identities, and self-representation. As a token of respect to these decisions ISPs should not throttle or otherwise discriminate against this traffic. So, in practice, the relationship between privacy tools and net neutrality is the inverse: We need rules that protect users from the possibility of ISPs forcing them to reveal some aspects of their identity they might consider to be a private matter.

Why shouldn't the FTC or other bodies ensure the principles of net neutrality are upheld?

The FCC has technical teams better prepared to understand how threats to the net neutrality principles actually materialize. Furthermore, the FTC could only carry out a reactive process on a case-by-case basis that would be costly, time consuming, and generate greater uncertainty than the general net neutrality rules put in place by the FCC through the Open Internet Order. The same could be said of the judiciary.